REMARKS

Claims 1-8 are pending in the application, with claims 1-8 having been amended hereby.

The claims have been carefully reviewed and amended with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present response.

Reconsideration is respectfully requested of the rejection of claims 1-8 under 35 U.S.C. § 102(b), as allegedly being anticipated by U.S. Patent No. 6,075,860 to Ketcham.

Applicants have carefully considered the comments of the Office Action and the cited reference, and respectfully submit that claims 1-8 are patentably distinct over the cited reference for at least the following reasons.

The present invention relates to a method for securely and conveniently distributing keys to subscribers in communications networks such as digital mobile radio networks. The keys are generated and stored in a security device provided at the mobile radio network end. Upon request by a subscriber, at least one key is allocated to the subscriber and transmitted via the mobile radio network to the subscriber's mobile station.

Ketcham, as understood by Applicants, relates to an apparatus and method for authentication and encryption of a remote terminal over a wireless link. An encrypted wireless communication channel is established between a remote terminal and a network server for facilitating the authentication

process. An authorized user presents an authentication card containing credentials including a user identifier and an authentication encryption key to a remote terminal. The remote terminal establishes a wireless communication channel with a network server which provides a firewall between unauthenticated users and a computer network. The network server and the remote terminal exchange encrypted information to verify the authenticity of each party, and the remote terminal and the network server each independently generate a data encryption key for use in establishing a secure encrypted wireless communication channel.

The Office Action states that Ketcham discloses, inter alia, a method for distributing keys wherein keys are generated in a security device provided at the mobile radio network end and are transmitted via the mobile radio network to a mobile station or terminal of a subscriber, whereby the transmitted keys are stored in the terminal or subscriber identity module (SIM) in the mobile station (see Office Action, p. 2, lns. 12-21). Applicants respectfully disagree.

As understood by Applicants, Ketcham discloses the use of a portable storage device, such as an authentication card, for storing information specific to an authorized user (see Ketcham, col. 6, lns. 34-41). The authentication card is a portable device such as a smart card that may be carried by an authorized user, and may include a GSM SIM (see id., col. 8, lns. 20-37).

The information stored on the authentication card

includes a mobile subscriber identifier (MSID) designating the assigned identity of the user, and an authentication encryption key that is used to securely authenticate the user and to generate a data encryption key for encrypted transmission over the wireless channel (see id.; col. 6, lns. 34-41).

The authentication keys of Ketcham are generated by an account generator which processes requests by authorized users (see id., col. 6, lns. 42-67). The account generator includes a key generator for generating the encryption key, and assimilates the MSID with the encryption key to provide an indexing designator for use by the network server for distinguishing among encryption keys (see id., col. 7, lns. 1-16).

Additionally, the account generator of Ketcham disseminates the MSID, coupled with authentication encryption key, to both the authentication card and to the network server (see id.; Figs. 2-3).

The identification information of Ketcham is read from the authentication card by insertion of the card into a card reader, which receives the MSID and key stored on the card in response to a card interrogation by the remote terminal (see id., col. 8, lns. 46-65; Fig. 5).

It is respectfully submitted, however, that Ketcham does not disclose or suggest transmission of the encryption key to the mobile terminal via the mobile radio network.

In contrast, in the present invention the keys are

generated and stored in a security device at the mobile radio network end, and are transmitted to a mobile station or terminal via the mobile radio network upon request, as recited in amended independent claim 1.

In an embodiment of the present invention, for example, the security server produces the keys, stores them in a data bank, and distributes the keys on request from a subscriber to the subscriber identity module in the mobile station and to the added value service nodes that may be used by the subscriber (see specification of the present application, p. 5, lns. 12-24). The short message service center in the mobile radio network transmits the keys in the form of short messages between the security server and the mobile station (see id.).

Furthermore, it is respectfully submitted that Ketcham does not disclose or suggest storage of the transmitted key in the terminal or subscriber identity module in the mobile station, as recited in independent claim 1.

Additionally, it is submitted that Ketcham does not disclose a method whereby a subscriber may request and store a plurality of keys at any time, and use the keys when required for authentication against a telecommunications service.

In contrast, in an embodiment of the present invention, the security server sends the key in a short message to the mobile station, where it is stored on the (U)SIM (see specification of the present application, p. 6, lns. 1-5). In this manner, the (U)SIM is utilized as a protected-access

medium to check, store, and use passwords or keys for authentication from a mobile radio network (see id., p. 2a, lns. 5-12).

Furthermore, the configuration of the above-described embodiment of the present invention allows the subscriber to request and store a plurality of keys, which may then be used as necessary. Each key may be assigned to a telecommunication service, for example, and each may selectively be used to gain access to its respective service.

It is respectfully submitted that Ketcham does not show or disclose a method for distributing keys to subscribers in digital mobile radio networks, comprising the steps of generating the keys in a security device provided at the mobile radio network end, requesting at least one key from the security device, and transmitting the at least one key via the mobile radio network to a mobile station or a terminal of a subscriber, wherein the generated keys are stored in the security device prior to transmission, the requesting step is performed by the subscriber, the transmitted key is allocated to the subscriber, and the transmitted key is stored in the terminal and/or in a subscriber identity module in the mobile station, as described above and as recited in amended independent claim 1.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that amended independent claim 1, and the claims depending therefrom, including claims 2-8, are patentable over the cited reference.

Withdrawal of the rejection of claims 1-8 under 35 U.S.C. § 102(b) is respectfully requested.

The references cited as of interest have been reviewed, but are not seen to show or suggest the present invention as recited in the amended claims.

Should the Examiner disagree, it is respectfully requested that the Examiner specify where in the cited document there is a basis for such disagreement.

The Office is hereby authorized to charge any fees which may be required in connection with this amendment and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Respectfully,

Dated: August 9, 2004

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

8/9/04

Norman H. Zivin Date
Reg. No. 25,385

Norman H. Zivin
Reg. No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036
(212) 278-0400
Attorney for Applicants